UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH ALLENWNC2@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE

Case No. 1:19 mj 70

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A of Attached Affidavit

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B of Attached Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251(a)	Production of child pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of child pornography
18 U.S.C. § 2252A(a)(2)	Receipt and distribution of child pornography

The application is based on these facts:

See Search Warrant Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Timothy K. Thiel, Task Force Officer, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/9/2019

Judge's signature

City and state: Asheville, North Carolina

W. Carleton Metcalf, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **ALLENWNC2@GMAIL.COM** THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, LLC	Case No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Timothy K. Thiel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheater Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer (TFO) with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I am currently assigned to HSI Hendersonville, North Carolina office. As part of my official duties, I have conducted and participated in investigations related to cyber-crimes and the sexual exploitation of children. I

have also received training and instruction in the field of investigating cyber related and child pornography crimes. I further have extensive experience in investigating cyber child exploitation cases to include the production, distribution, and transportation of child pornography images and videos via the internet. As part of my duties and responsibilities as an HSI Task Force Officer, I am authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2251, et seq.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, § 2252A(a)(1), transportation of child pornography, Title 18, United States Code, § 2251(a) production of child pornography, Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography, Title 18, United States Code, § 2252A(a)(2) receipt and distribution of child pornography have been committed via the **ALLENWNC2@GMAIL.COM** Google account. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court for the Western District of North Carolina: is "a district court of the United States . . . that has jurisdiction over the offense being investigated."

PROBABLE CAUSE

6. On Sunday, July 28, 2019, the Hendersonville Police Department was dispatched to a residence located in Hendersonville, North Carolina, within the Western District of North Carolina due to a report by the residents that their son had possibly been sexually exploited.

7. At the residence, it was reported by the minor victim's parents that minor victim one (MV1), their 13-year-old son, was having inappropriate and sexually explicit conversations with an adult male who is an instructor at the taekwondo academy that MV1 attends. The suspect was identified as Jeffrey Allen BULEY.

8. During the investigation, I discovered that MV1 was communicating with BULEY via an app called Discord.

9. On Sunday, July 28, 2019 MV1's mother reported that she was calling for MV1 to come upstairs because dinner was ready, but MV1 repeatedly did not answer her. MV1's mother stated that when she went upstairs to look for MV1, she found him in the bathroom with the door closed. MV1's mother stated that as she approached the bathroom door, she heard MV1 talking as if he was on the telephone and heard another male's voice. MV1's mother stated she heard MV1 make a reference to sex toys and after hearing such, she became suspicious and knocked on

the door. MV1's mother stated that MV1 quickly disconnected the call and put down the device he was using.

10. MV1's mother stated she began looking through the device and discovered that MV1 had been using Wi-Fi to make telephone calls.

11. MV1's mother also discovered the Discord app but saw that the most recent record had been deleted.

12. MV1's mother and father then went to MV1's desktop computer and opened the Discord app and located messages between MV1 and a user utilizing the screenname "allenwnc."

13. MV1 explained to his parents that the user utilizing the screenname "allenwnc" was actually Jeffrey Allen BULEY. MV1 also provided the email address "allenwnc@yahoo.com" as an email address used by BULEY.

14. MV1 stated he began communicating with BULEY via the Internet and apps around August 2018 (when MV1 was then 12 years old) and began communicating with BULEY on the Discord app around April 2019.

15. MV1 stated that while communicating with BULEY via the Discord app, and possibly other apps, BULEY and MV1 would exchange nude photographs of each other, focusing on each other's genitalia. MV1 also stated BULEY would make specific requests for nude photographs of MV1's genitalia and MV1 would send the requested photos to BULEY via the Discord app or other apps.

16. MV1 reported incidents where he was alone with BULEY and stated that BULEY had sexually molested him. MV1 stated BULEY watched him completely undress to the point where MV1 was fully nude. MV1 also reported that BULEY has exposed his penis to MV1 and

began masturbating in front of him and then also touched MV1's penis and began masturbating MV1. MV1 reported that BULEY has also touched his penis on the outside of his clothing.

17. On July 28, 2019, I met with MV1's parents and seized three devices belonging to MV1, an Apple iPod touch, a Samsung laptop, and a Hewlett-Packard computer tower.

18. Utilizing a Department of Homeland Security U.S. Immigrations and Customs Enforcement Consent to Search form, MV1's mother consented to HSI TFO Thiel seizing and searching the items mentioned above.

19. On Monday, July 29, 2019 I accessed MV1's account on the Discord app and located the following messages which occurred on Sunday, July 28, 2019 between MV1 (using screen name "DVM") and BULEY (using screen name "allenwnc"):

20. DVM: sup mate (1:05PM)

21. allenwnc: I think we're both cleaning up at the same time (5:03PM)

22. DVM: No I'm waiting for u (5:04PM)

23. To get a bath

24. allenwnc: Okay I can pull over for like 5 minutes somewhere hold on (5:04PM)

25. DVM: Ok (5:04PM)

26. allenwnc: Ok go (5:08PM)

27. DVM started a call (5:08PM)

28. MV1 stated the call placed was a video chat between himself and BULEY. MV1 stated that he was in his bathroom, fully nude, sitting in the bathtub showing BULEY his penis. MV1 stated this was the first time that he has chatted with BULEY while in the bathtub and stated that he usually video chats with him when he is taking a shower. MV1 stated BULEY was in a

vehicle and had pulled over on the side of the road to video chat with him. MV1 stated that BULEY was using some sort of cellular smart phone at the time.

29. MV1 stated that he and BULEY routinely video chat via the Discord app. MV1 stated that he and BULEY regularly show each other their penises, masturbate and ejaculate. MV1 stated there have been times when BULEY has directed him what to do or what he would like to see MV1 do on the video chat.

30. On Tuesday, July 30, 2019, I applied for and was granted a federal search warrant, 1:19-MJ-70, by the Honorable United States Magistrate Judge W. Carleton Metcalf, of the Western District of North Carolina. The search warrant was issued for 714 Clearview Drive, Hendersonville, North Carolina; and granted permission to search for items related to production, possession, receipt and distribution of child pornography.

31. On Tuesday, July 30, 2019 at approximately 1800 hours (EST) HSI Special Agents (SA) and Task Force Officers (TFO) in conjunction with the United States Marshals Service (USMS), Hendersonville Police Department (HPD), and the Henderson County Sheriff's Office (HCSO), executed the federal search warrant at 714 Clearview Drive, Hendersonville, North Carolina.

32. As agents were entering the residence located at 714 Clearview Drive, Hendersonville, North Carolina to execute the search warrant, BULEY exited a residence next door which is located at 708 Clearview Drive, Hendersonville, North Carolina. BULEY was apprehended and taken into custody for three outstanding warrants for violations of North Carolina state law pertaining to the conduct describe above.

33. Agents then conducted a protective sweep of the residence and while doing so discovered an open laptop on a desk in a bedroom that was in plain view. Agents stated they

observed a live video chat stream but could not provide details as to who BULEY was video chatting with.

34. Utilizing a Department of Homeland Security U.S. Immigrations and Customs Enforcement Statement of Rights form, BULEY was advised of his rights which he waived in writing.

35. Utilizing a Department of Homeland Security U.S. Immigrations and Customs Enforcement Consent to Search form, BULEY then signed and gave consent for agents to search the following items which were inside the residence located at 708 Clearview Drive, Hendersonville, North Carolina:

LG cell phone (Model: LMQ710MS)

Samsung Chromebook (serial number: 0Q9T91H5301276A)

HP Pavilion p2 Series computer (model: ps-1013w) (serial number: 3CR14008JQ)

36. While Computer Forensic Agents (CFA) were conducting the search of the Samsung Chromebook (serial number: 0Q9T91H5301276A), CFAs and I discovered a .GIF file of a nude pubescent male masturbating and ejaculating in the Google drive account associated with Google account **ALLENWNC2@GMAIL.COM.**

37. A .GIF file stands for the file extension, Graphic Interchange Format. Some .GIF files are live photographs or in other terms, videos of very short duration.

38. Samsung Chromebooks are a new type of computer designed with Chrome OS that have Google cloud storage instead of a hard drive. When using the computer, it appears the files are on the computer like a traditional operating system, such as Windows or Mac operating systems, however they are stored on a cloud server.

BACKGROUND CONCERNING GOOGLE

39. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access and cloud-based storage to the public. Google allows subscribers to obtain email accounts at the domain name www.gmail.com, like the email account listed in Attachment A. After subscribers obtain the Google account, they are then provided the variety of online services Google provides.

40. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

42. In my training and experience, Google generally asks their subscribers to provide certain personal identifying information when registering for a Google account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including

any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

43. In my training and experience, Google typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

44. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

BACKGROUND CONCERNING GOOGLE DRIVE

45. Google Drive is a cloud storage service with its main purpose being to expand the user's ability to store files beyond the limits of a computer's hard drive.

46. Users sign up for Google Drive by creating a Google account, it is an online service provided to the user for creating a Google account. Google provides users 15GB of free cloud storage for creating a Google account. This free space is shared between Google Drive, Google Photos and Gmail (Google's email).

47. Google Drive can store any kind of file to include but not limited to photographs, videos, documents, etc. Users can save email attachments sent to them through Gmail directly to Google Drive.

48. Users are able to access Google Drive through an internet browser, desktop file system or a mobile device such as a cell phone or tablet.

49. In my training and experience, such information may constitute evidence of the crimes under investigation.

50. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

51. As explained herein, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described below, providers typically log the Internet Protocol (IP) addresses from which users access the account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

52. On July 31, 2019, a preservation letter was sent to Google requesting the preservation of content for Google account **ALLENWNC2@GMAIL.COM**. Google representatives responded stating that they received the request.

LEGAL AUTHORITY

53. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711 and 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a "district court of the United States . . . that – (i) has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

CONCLUSION

54. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REVIEWED BY ASSISTANT UNITED STATES ATTORNEY DAVID A. THORNELOE

Respectfully submitted,

Timothy K. Thiel
Task Force Officer
Homeland Security Investigations

Subscribed and sworn to before me on August 9th, 2019

W. CARLETON MATCALF
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF NORTH CAROLINA

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with **ALLENWNC2@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google, an email provider headquartered at 1600 Amphitheater Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on July 31, 2019, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, **ALLENWNC2@GMAIL.COM**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. The contents and all files to include the associated metadata located within the Google Drive account, including any deleted or files residing in the trash connected to the **ALLENWNC2@GMAIL.COM**, including any and all log data for that Google Drive account.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized;

e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

g. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within up to 14 days of the issuance of this warrant.

Google shall disclose responsive data, if any, by sending to:

HSI TFO Timothy K. Thiel
518 6th Ave West
Hendersonville, NC 28739

Google shall use the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, § 2252A(a)(1), transportation of child pornography and Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography, those violations involving Jeffrey Allen BULEY and occurring after the date of the creation of the email account, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The transportation of child pornography to included distribution and receipt of child pornography images and/or videos via the internet and email. Conversations between BULEY and others related to child pornography trading and sharing.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).